PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/08

A1

(11) International Publication Number: WO 99/14887

(43) International Publication Date: 25 March 1999 (25.03.99)

(21) International Application Number: PCT/GB98/02774

(22) International Filing Date: 14 September 1998 (14.09.98)

(30) Priority Data:
9719726.3 16 September 1997 (16.09.97) GB

(71) Applicant (*for all designated States except US*): SIMOCO INTERNATIONAL LIMITED [GB/GB]; P.O. Box 24, St. Andrews Road, Cambridge CB4 1DP (GB).

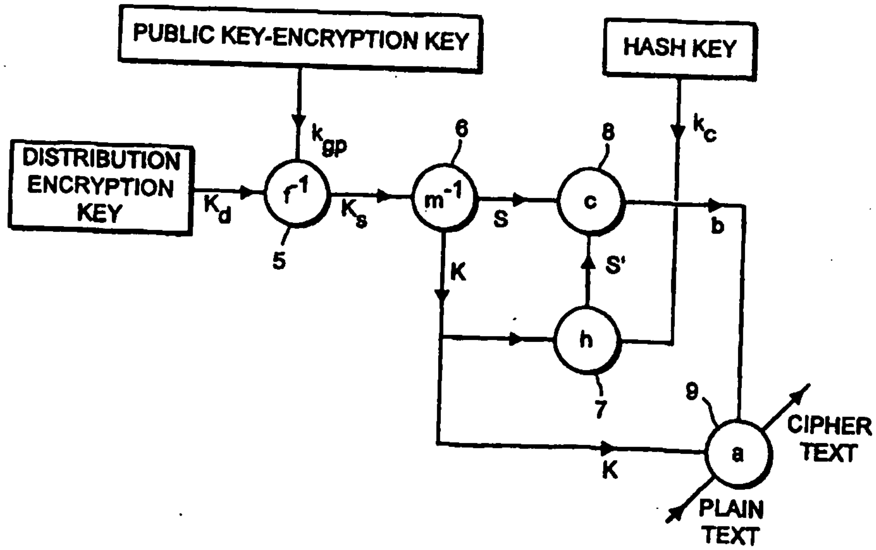
(72) Inventor; and
(75) Inventor/Applicant (*for US only*): RAYNE, Mark, Wentworth [GB/GB]; 5 St. James Close, Stretham, Nr. Ely, Cambridgeshire CB6 3ND (GB).

(74) Agent: FRANK B. DEHN & CO.; 179 Queen Victoria Street, London EC4V 4EL (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ENCRYPTION METHOD AND APPARATUS WITH VARIABLE ENCRYPTION STRENGTH



(57) Abstract

An encryption method and apparatus in which a cryptographic encryption key (K) for use to encrypt or decrypt communications is first derived from a cryptographic key (K_d) provided by a user. The derived encryption key is used to encrypt or decrypt communications at a selected level of encryption strength. The level of encryption strength is selected in accordance with whether or not the cryptographic key provided by the user has a particular property, such as including a particular sequence of bits, dividing exactly by a particular number, or whether a particular cryptographic check value (S) can be derived from it. A method and apparatus for generating suitable cryptogrpjhic keys are also described.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

ENCRYPTION METHOD AND APPARATUS WITH VARIABLE ENCRYPTION STRENGTH

The present invention relates to an encryption method and apparatus and in particular to such a method and apparatus which can be arranged to prevent unauthorised users of an encryption device from being able to obtain strong encryption with that device.

There is now an increasing need for highly secure end-to-end encryption in communication networks. This is particularly required by military and public safety users of radio and telephone communications, but high grade end-to-end encryption devices are also becoming increasingly available to the general public.

Such encryption devices typically use a cryptographic key, for example in the form of a binary number, input by a user of the device to encrypt messages that the user sends with the communications apparatus in which the encryption device is incorporated, as is well known in the art. Examples of such encryption methods include secret key encryption and public key encryption.

As strong encryption comes into more general use, there is an increasing likelihood that devices providing it will get into the hands of unauthorised users, such as criminals, who will then be able to use these devices with their own keys to encrypt their own communications. This could create difficulties for law enforcement agencies who are legitimately intercepting such communications by unauthorised users, because they will not know the encryption keys being employed and may be unable otherwise to decrypt the communications due to the strength of the encryption.

To counter this, national governments are increasingly demanding the use of key escrow, whereby any persons wishing to employ strong end-to-end

encryption are expected to lodge their keys with a trusted third party (TTP) who will keep the keys secret except when required to release them by an authorised law enforcement or other agency. In this way, lawful users of encryption are ensured of communications confidentiality, but unauthorised users' communications using escrowed keys can, it is hoped, be decrypted if necessary because the relevant key can be retrieved from the trusted third party.

However, in practice unauthorised users may be able to create secretly their own keys for use with the strong encryption devices that they acquire, which will not then be known by the trusted third party under the key escrow arrangement. In that case, law enforcement agencies could still be unable to decrypt the unauthorised users' communications.

According to a first aspect of the present invention, there is provided an encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for deriving from a cryptographic key input by a user of the apparatus a cryptographic encryption key for use to encrypt or decrypt communications;

means for determining whether the input cryptographic key has a particular property;

means for selecting one of said two or more levels of encryption strength on the basis of the determination; and

means for encrypting or decrypting communications at the selected level of encryption strength using the derived encryption key.

According to a second aspect of the present invention, there is provided a method of encrypting or decrypting communications comprising:

deriving from a first cryptographic key a cryptographic encryption key for use to encrypt or decrypt communications;

determining whether the first cryptographic key has a particular property;

selecting a level of encryption strength on the basis of the determination; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

In the present invention, rather than using the cryptographic key input by a user (or a first cryptographic key) directly to encrypt or decrypt communications, an encryption key is derived from the input (or first) cryptographic key, and the strength of the encryption effected using the derived encryption key is then selected in accordance with whether or not the input (or first) key has a particular property. The present invention thus switches between two or more levels of encryption strength (such as high and low strength encryption modes) on the basis of a particular property of the input (or first) cryptographic key.

The present invention can therefore be arranged to provide strong encryption for an authorised user using an authorised key (which would normally be escrowed), but only weaker or no encryption with an unauthorised key as might be input by an unauthorised user. The authorised input key would have the particular predetermined property which selects high strength encryption. However, unauthorised users wishing to use their own unauthorised keys, would not know the relevant property, and thus would be unable to obtain strong encryption.

The encryption key can be derived from the input cryptographic key in a number of ways, as will be appreciated by those skilled in the art. It could, for example, comprise the entire input cryptographic key in the form that it is input. However, the encryption key preferably differs from the input cryptographic key. It could, for example, be derived by taking some or all of

the bits of the input key in some predetermined manner. For example, a predetermined number of bits from a predetermined part of the input key (such as one end of the key), or bits from more than one part of the input key (such as every other bit of the key), could be used to form the encryption key. The bits could also be reordered in a predetermined manner before or after taking them from the input key, if desired.

The particular property of the input cryptographic key should preferably be such that an authorised input cryptographic key can readily be arranged to have it, but it is unlikely that any unauthorised key could by chance possess it; otherwise, it can be selected as desired. For example, the property could be whether the input key includes a particular sequence of bits, is exactly divisible by a particular number, or whether it belongs to a particular mathematical series (such as the Fibonacci series).

The particular property of the input cryptographic key is preferably a concealed property of the key which is not readily apparent from an authorised input key (unlike, for example, the length of the key).

Most preferably, the property is derived by taking or using bits of the input key in a predetermined manner. This makes the property much less apparent and more difficult to guess from the input key alone.

Whether or not the input key has a particular property can be determined in a number of ways and will depend on the property concerned. For the above examples, the input key could be compared with a stored sequence of bits, the particular number could be divided into the input key, or the input key could be compared with known members of the mathematical series (stored, for example, in a memory in the encryption device), respectively.

Preferably, the level of encryption strength is selected on the basis of whether or not the input key

has the particular property. For example, stronger (or the maximum) level of encryption strength could be selected if the input key has the particular property, and a second level of encryption strength (e.g. weak or no encryption) selected if the input key does not have the particular property.

In a particularly preferred embodiment of the present invention, the particular property according to which the encryption strength is selected is whether or not an appropriate cryptographic check value is derivable from the cryptographic input key. In this embodiment, the present invention will therefore comprise means or a step of deriving a cryptographic check value from the input cryptographic key, and the level of encryption strength will be selected on the basis of the derived check value. This embodiment of the present invention is thought to be particularly advantageous, in that it will be more difficult for an unauthorised user to determine an input cryptographic key from which a check value which selects higher strength encryption can be derived.

Thus, according to a third aspect of the present invention, there is provided an encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for deriving from a cryptographic key input by a user of the apparatus a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

means for selecting one of said two or more levels of encryption strength on the basis of the derived check value; and

means for encrypting or decrypting communications at the selected level of encryption strength using the derived encryption key.

According to a fourth aspect of the present invention, there is provided a method of encrypting or

decrypting communications comprising:

deriving from a cryptographic key a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

selecting a level of encryption strength on the basis of the derived check value; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

In these aspects of the present invention, an encryption key and a cryptographic check value (which can also be referred to a "certificate" or "signature", as is known in the art) are derived from the input key, and the strength of the encryption effected using the derived encryption key is then selected in accordance with the derived check value. These aspects of the present invention thus switch between two or more levels of encryption strength on the basis of information (the check value) carried by the input cryptographic key.

The check value can be derived from the input cryptographic key in a number of ways, as will be appreciated by those skilled in the art. It could, for example, be derived by taking several or all of the bits of the input key in some predetermined manner. For example, a predetermined number of bits from a predetermined part of the input key (such as one end of the key), or bits from one or more parts of the input key (such as every other bit of the key), could be used to form the check value. In such an arrangement the remaining bits of the input key could be used to form the encryption key. The bits could also be reordered in a predetermined manner before or after taking them from the input key, if desired.

The derived check value can be used to select the strength of the encryption in many ways. For example, the derived check value could be used to calculate a number or other information which is then used to select

the level of encryption strength. However, the derived check value is preferably compared with one or more other check values and the encryption strength selected on the basis of that comparison. For example, a first (e.g. stronger or the maximum) level of encryption could be selected if the derived check value matches one of the other comparison check values, and a second level of encryption (e.g. weaker or no encryption) selected if the derived check value does not match any of the other comparison check values.

The other check values for comparison with the derived check value can be predetermined and stored in the encryption apparatus. However, in this arrangement it may be possible for someone to read the comparison check values in the encryption device.

The other check value or values for comparison with the derived check value are therefore preferably derived from the input cryptographic key in a predetermined manner. In a particularly preferred such arrangement, the check value derived from the input key is compared with a further check value derived from the derived encryption key and the strength of the encryption is selected on the basis of the result of that comparison (for example whether or not a match is found). This arrangement makes it particularly difficult for an unauthorised user to accidentally input, or to deduce, a key which will provide strong encryption, since not only must the input key provide the correct check value, it must also include an encryption key from which the correct further check value will be derived.

The further check value could be derived by taking predetermined bits of the derived encryption key in a particular order. However, it is preferably derived from the derived encryption key by performing a predetermined cryptographic function on the derived encryption key, as this makes it more difficult still for an unauthorised user to produce their own input keys

which will provide strong encryption. It is preferably derived by performing an irreversible cryptographic hash function on the derived encryption key.

It is believed that varying the strength of encryption in accordance with the results of a comparison between a cryptographic check value derived from an input cryptographic key and a further cryptographic check value derived from an encryption key derived from the input cryptographic key is particularly advantageous.

Thus according to a fifth aspect of the present invention, there is provided an encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for deriving from a cryptographic key input by a user of the apparatus a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

means for deriving from the derived encryption key a further cryptographic check value;

means for comparing the derived check value and the further check value;

means for selecting one of said two or more levels of encryption strength on the basis of the comparison; and

means for encrypting or decrypting communications at the selected level of encryption strength using the derived encryption key.

According to a sixth aspect of the present invention, there is provided a method of encrypting or decrypting communications, comprising:

deriving from a cryptographic key a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

deriving from the derived encryption key a further cryptographic check value;

comparing the derived check value and the further

check value;

selecting a level of encryption strength on the basis of the comparison; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

The different levels of encryption strength could, for example, comprise full (or maximum) available strength encryption or no encryption (or preventing the device from working) at all. For example, full (maximum) strength encryption could be provided if the input key has the particular property (e.g. if the derived check value matches an authorised check value (or matches the derived further check value)), but no encryption provided or the device refuse to operate at all (i.e. produce no cipher text or plain text output) if the input key does not have the particular property (e.g. if the derived check value does not match an authorised check value (or the derived and further check values do not match)).

However, in a particularly preferred embodiment, the encryption strength is varied between full (maximum), or higher, strength encryption and weaker encryption (but still some level of encryption rather than no encryption at all) on the basis of the determination of whether the input key has the particular property (e.g. on the basis of the derived check value). This can be advantageous because it makes it more difficult for an unauthorised user who uses a key which does not have the particular property (e.g. provide a check value) necessary for full strength encryption to realise that their communications are not being encrypted fully.

In another preferred embodiment, three or more different levels of encryption strength are provided. This could enable the same encryption device to provide full strength encryption for, for example, government

agencies, weaker encryption for private individuals or businesses using authorised escrowed keys, and even weaker or no encryption for users of unauthorised keys.

In this embodiment each authorised level of encryption strength could have its own particular property, such as a number by which the input key must be exactly divisible, or a mathematical series to which the input key must belong. Alternatively, each authorised level of encryption strength could have its own individual authorised check value.

The level of encryption strength could then be selected in accordance with which property the input key has. For example, it could be selected by comparing the derived check value with the relevant number of comparison check values and selecting the encryption strength permitted by whichever comparison check value the check value derived from the input key matches. Alternatively, multiple further check values could be derived from the derived encryption key (for example by performing a number of hash functions on the derived encryption key and/or by using a number of different hash keys) and the derived check value compared with each of those further comparison check values and the encryption strength selected on the basis of those comparisons.

The strength of encryption can be changed in various ways, as is well known in the art. One way to do this would be by altering the derived encryption key, for example to reduce its effective length to a value which makes a key search feasible (e.g. by setting a number of bits to a fixed value, or by repeating sequences of bits). Alternatively, or additionally, the encryption algorithm could be altered to facilitate cryptanalysis. In the case of the DES or IDEA algorithms, for example, the number of "rounds" could be drastically reduced, or the DES "S Box" and permutations could be modified. One or more of these alterations

could be put into effect whenever the input key does not have the relevant particular property (e.g. the derived check value does not indicate that full strength encryption is authorised).

Although it has been described above with respect to an encryption apparatus and method, the present invention also extends to the generation of authorised input keys including check values for use with the encryption apparatus and method of the present invention.

The authorised input key should include an encryption key and a cryptographic check value combined in such a manner that they will be correctly derived by the encryption apparatus for which the input key is intended. Thus the input key is basically generated by combining a cryptographic encryption key and a cryptographic check value in a manner complementary to the way in which the encryption key and check value are to be derived from the input key. The method of combination will therefore generally speaking be the reverse of the intended process for deriving the encryption key and check value from the input key (although conversely the method of deriving the encryption key and check value from the input key could be predetermined by the method of generating an authorised input key from a given encryption key and an authorised check value).

Thus, for example, the encryption key and check value could be combined by appending the bits of the check value to, or interleaving them with, the bits of the encryption key, in the converse manner to the way the encryption key and check value are derived from the input key in the encryption apparatus or method.

The encryption key itself can be any form of encryption key known in the art, such as keys suitable for use in symmetrical, secret key cryptography or in public key cryptography. It could, for example,

comprise a randomly generated key of a desired length, or a user's secret, public or private key.

The check value should be such that it readily identifies an authorised input key. It could for example comprise a predetermined binary word. However, this arrangement is not preferred, since if an unauthorised user manages to determine the binary word, he may then be able to combine it with his own unauthorised encryption keys to allow him to use strong encryption with the encryption device.

In a particularly preferred embodiment therefore, the check value is derived in a predetermined manner from the encryption key. This helps to ensure that identifying the check value of one key does not automatically provide a check value that will work for all keys. This method of generating a check value is particularly suited for use with the above aspects of the present invention in which a further comparison check value is derived from the derived encryption key. In such cases, the ways of generating the check value and deriving the further comparison check value are preferably identical.

The check value could be generated from the encryption key by, for example, taking predetermined bits of the encryption key in a particular order. However, it is preferred that the check value is generated cryptographically from the encryption key, as this makes it harder to determine how to generate a correct check value for any encryption key, for example by performing a cryptographic certification function on the encryption key.

In a particularly preferred such embodiment, the check value is generated by performing an irreversible cryptographic hash function on the encryption key, as this makes it more difficult still to determine how to generate a correct check value for any encryption key.

In the case where a number of check values are

required (for example, if three or more levels of encryption are provided), each check value can be generated from the encryption key in a different predetermined manner. For example, different hash functions could be performed on the encryption key to provide different check values and/or a different hash key could be employed for each level.

The check value is preferably of sufficient length that it is extremely improbable that a correct check value can be created by accident. It should therefore generally speaking be as secure as the encryption key with which it is combined. Thus the check value is preferably the same length as or a similar length to the encryption key.

The provision of a cryptographic key comprising an encryption key and a check value which is derived cryptographically from the encryption key is believed to be particularly advantageous, in that it provides a certificated cryptographic key from which it is particularly difficult to deduce correct check values for other encryption keys.

Thus according to a seventh aspect of the present invention, there is provided a method of generating a cryptographic key having a check value for authorising its validity, comprising:

generating an encryption key for use to encrypt or decrypt communications;

generating a check value from the encryption key by performing one or more cryptographic functions on the encryption key; and

combining the encryption key and check value to form a certificated cryptographic key.

According to an eighth aspect of the present invention, there is provided an apparatus for generating a cryptographic key having a check value for authorising its validity, comprising:

means for generating an encryption key for use to

encrypt or decrypt communications;

means for generating a check value from the encryption key by performing one or more cryptographic functions on the encryption key; and

means for combining the encryption key and check value to form a certificated cryptographic key.

According to a ninth aspect of the present invention, there is provided a cryptographic key comprising the combination of an encryption key and a check value generated from the encryption key by performing one or more cryptographic functions on the encryption key.

In a particularly preferred arrangement of these aspects of the present invention, the generated input key is further encrypted before it is distributed to authorised users. Correspondingly, the encryption apparatus and method of the first to sixth aspects of the present invention preferably therefore further include means for or a step of decrypting an input key before the encryption key and particular property (e.g. check value) are determined (or derived) therefrom.

This additional encryption makes it harder still for an unauthorised user to generate their own key that will provide strong encryption, since in this arrangement the input key must provide a key which when decrypted will provide an encryption key and a correct property (e.g. check value). It could be for example that an unauthorised user of an encryption device incorporating the present invention would be able to extract from the device sufficient information to be able to derive their own check value that would provide a strong encryption or may have obtained knowledge of the certification algorithm in some other way. However, even in that case they will still not know how to correctly encrypt their bogus key such that when decrypted by the encryption device, the device then derives from it an encryption key and a correct check

value for strong encryption.

Thus according to a tenth aspect of the present invention, there is provided a method of generating a cryptographic key for distribution to users of encryption devices, comprising:

combining a cryptographic encryption key with a cryptographic check value; and

encrypting the combined key to provide the cryptographic key.

According to an eleventh aspect of the present invention, there is provided an apparatus for generating a cryptographic key for distribution to users of encryption devices, comprising:

means for combining a cryptographic encryption key with a cryptographic check value; and

means for encrypting the combined key to provide the cryptographic key.

According to a twelfth aspect of the present invention, there is provided a cryptographic key comprising an encrypted version of the combination of a cryptographic encryption key and a cryptographic check value.

According to a thirteenth aspect of the present invention, there is provided an encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for decrypting a cryptographic key input by a user of the apparatus using a predetermined decryption key;

means for deriving from the decrypted input key a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

means for selecting one of said two or more levels of encryption strength on the basis of the derived check value; and

means for encrypting or decrypting communications at the selected level of encryption strength using the

derived encryption key.

According to a fourteenth aspect of the present invention, there is provided a method of encrypting or decrypting communications comprising:

decrypting a cryptographic key using a predetermined decryption key;

deriving from the decrypted key a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

selecting a level of encryption strength on the basis of the derived check value; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

The encryption used for the input key can be any form of encryption known in the art.

It could, for example, be encrypted by symmetrical secret key cryptography with the corresponding encryption device then using the relevant secret key to decrypt the input key before deriving the encryption key and check value therefrom. In this arrangement the secret key is preferably stored in an unreadable form in the encryption device, as is known in the art, as this stops an unauthorised user from being able to read the secret key from the encryption device and thus perhaps generate their own unauthorised key. The secret key could, for example, be stored inside a memory which can be wiped by a tamper detection circuit when it detects an attempt to read the memory.

In a particularly preferred embodiment, the input key is encrypted using a reverse form of public key cryptography. The key generator uses his private key to encrypt the input key and the encryption device then uses the key generator's public key to decrypt it. This is a more secure arrangement because even if an unauthorised user manages to read the public key in the encryption device, he will still not know the private

key necessary to create the input key properly.

In this arrangement it is preferred that the public key in the encryption device be stored in such a way that it is unalterable in the encryption device, as is known in the art, as this prevents an unauthorised user from putting their own public key in the encryption device. The public key could, for example, be hard coded in an unalterable way into the encryption device, or stored inside a memory which is disabled (such that it can't be rewritten to) if tampering is detected. Alternatively, it could be stored in two separate memory locations and checks periodically made to see that they match, with the memory being wiped if they don't match. The public key is preferably also unreadable in the encryption device, although as noted above, this is not essential.

Further levels of encryption to the input key can be added, if desired. For example, as well as encrypting it with the key generator's key, that encrypted key could be further encrypted with an individual user's key (either by secret key encryption or public key encryption) such that the key can only be used by the individual for whom it is intended.

A number of preferred embodiments of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:-

Figure 1 shows a first embodiment of the generation of an authorised input key in accordance with the present invention;

Figure 2 shows a first embodiment of an encryption device in accordance with the present invention;

Figure 3 shows a second embodiment of the generation of an authorised input key in accordance with the present invention; and

Figure 4 shows a second embodiment of an encryption device in accordance with the present invention.

Figure 1 illustrates one method of generating an authorised input key in accordance with the present invention. The key generator or provider firstly generates a random encryption key K of length n_a required by the encryption algorithm using a random key generator 1.

A cryptographic check value (or key certificate or key signature) S of length n_b is then generated by check value generator 2. The check value generator 2 carries out a cryptographic certification irreversible hash function h on the encryption key K under the control of a hash key K_c, to provide the check value S. It is desirable to make the check value of sufficient length to make it extremely improbable that a correct check value can be created by accident. It is wise therefore to make the check value S of a similar length to the encryption key K.

The check value S is then appended to the encryption key K (or may be inserted or interleaved into K at specific bit locations) by combining means 3 in accordance with a mixing function m to create a certificated key K_s, of length $n_a + n_b$.

The certificated key K_s is then encrypted with the key generator's private encryption key, k_{gs}, using the reverse public key encryption algorithm f, by encryption means 4 to generate a distribution key K_d. This key K_d is the key that is provided to authorised users by the key generator, and would also be provided to a trusted third party under key escrow.

If it is required to restrict the use of a distribution key to individual encryption devices, key K_d may be further encrypted with a key unique to the individual encryption unit (not shown). This helps to protect key K_d from being used by some other person who has an encryption device holding the key generator's public key, should key K_d fall into the wrong hands.

Figure 2 shows an embodiment of an encryption

device in accordance with the present invention and in particular how an input key is authenticated inside the user's encryption device.

The user would firstly input the distribution key K_d into the encryption device. Key K_d would then be decrypted using an individual encryption device's decryption key, if individual encryption has been applied (not shown).

The input key K_d is then decrypted by decryption means 5 using the public key decryption algorithm f^{-1} (which is the inverse of f) and the key generator's public key k_{gp} to derive the certificated key K_s.

The derived key K_s is then fed to a dividing unit 6 which performs a dividing function m^{-1} (which is the inverse of m) on the certificated key K_s to derive the encryption key K and check value S.

Check value generator 7 of the encryption device then creates a further comparison check value S' from the derived encryption key K using the same certification function h and key K_c as were used to generate the check value S from the encryption key K by the check value generator 2.

Comparator 8 then compares the derived check value S and the further comparison check value S' and outputs a signal b whose value depends on whether the two check values are equal. Signal b controls the level of encryption strength provided by encryption means 9. If the two check values agree, signal b selects a strong encryption mode; if not, it selects a weak encryption mode.

Encryption means 9 encrypts plain text communications input to it using the derived encryption key K in accordance with a variable-strength encryption algorithm a, at the strength level determined by the signal b.

The encryption algorithm a can be any such algorithm known in the art, such as the DES or IDEA

algorithm. The strength of the encryption can be changed in various ways. For example, the encryption key K could be altered to reduce its effective length to a value which makes a key search feasible (for example by setting a number of bits to a fixed value, or repeating sequences of bits). Alternatively, the encryption algorithm could be altered to facilitate cryptanalysis. In the case of the DES or IDEA algorithms, for example, the number of "rounds" could be drastically reduced, or the DES "S Box" and permutations could be modified. Either or both of these alterations can be put into effect whenever the signal b indicates that the key does not carry a valid check value from the key provider.

The situation of an unauthorised user will now be considered. The unauthorised user, if unable to tamper with the encryption device, needs to furnish it with a key K_d which contains within it a check value which will cause the encryption device to use strong encryption. However, the unauthorised user should not have a knowledge of certification function h and hash key K_c, so will be unable to create a valid check value. However, the method of calculating the check value from the encryption key K is stored in every encryption device served by a particular authorised key generator, and it is possible therefore that an unauthorised user will find a means of extracting this information (e.g. by dissecting (and thereby destroying) an encryption device) and use it to produce forged check values S to correspond with his own invented key K. However, even in that event, no encryption device holds the authorised key generator's secret key k_{gs}, so it will not be possible for an unauthorised user to create a distribution key K_d which will yield a valid check value when decrypted with k_{gp}.

Note that it is desirable to make it very difficult for an unauthorised person to change the value of k_{gp}

inside the encryption device, as otherwise it could be changed to be the public key of an unauthorised user, who could then use their own secret key to enable them to bypass the key escrow mechanism. The key K_{gp} can be made unalterable by any means known in the art. For example, the key k_{gp} could be hard coded in an unalterable way into the encryption device.

It should also be noted that algorithm f does not have to be a public key algorithm, but could be a private key, symmetric algorithm. However, in this case it is desirable to make the key not only unalterable, but also unreadable inside the encryption device, as otherwise an unauthorised user could use this key and the check value to generate a valid distribution key K_d which has not been escrowed.

It is also desirable to ensure that it is not possible for anyone to bypass the key decryption means 5. Furthermore, the encryption device should be arranged such that it is not practical for a would-be user to modify, avoid or override the variable encryption strength control mechanism. Thus the encryption device preferably should be tamper-proof in general. Tamper protection can be achieved by encapsulating all functions shown in Figure 2, and their interconnections, in an integrated circuit, so that access can only be obtained to signals K_d, K_s, K and a by breaking open the device. The surface layers of the active encapsulated device should be covered by an additional tamper detection layer (for example a conductive grid, or a conductive spiral of known inductance and capacitance) such that the device can detect an attempt to probe through to lower layers and refuse to operate. The user's key and hash keys can be further protected by an anti-tamper switch in a box containing the device; if the box is opened, the keys are erased.

Figures 3 and 4 show alternative embodiments of

authorised input key generation and an encryption device in accordance with the present invention. These embodiments are similar to those shown in Figures 1 and 2, and thus the description above in relation to Figures 1 and 2 applies equally to the embodiments shown in Figures 3 and 4, where appropriate. Like reference numerals and symbols have been used in Figures 3 and 4 to denote the same features as appear in Figures 1 and 2.

The authorised input key generation shown in Figure 3 is identical to that shown in Figure 1, except that encryption means 10 further encrypts the distribution key K_d using encryption function u and encryption key K_u before the key is distributed to a user, to produce a user encrypted distribution key K_e. Encryption key K_u will typically be a key specific to an individual or particular group of users to help ensure that only that individual or group of users can use the distributed key. Key K_u will therefore usually be a user's (or user group's) secret key or public key and function u will use secret or public key encryption, respectively.

The encryption device shown in Figure 4 corresponds closely to that shown in Figure 2, but is adapted to use a key K_e as produced by the generation method of Figure 3. Thus the encryption device firstly includes additional decryption means 11 which uses decryption function u^{-1} (the reverse of u) and the corresponding user's decryption key K_u to decrypt the user encrypted distribution key K_e to re-derive the distribution encryption key K_d.

The device shown in Figure 4 also includes the possibility of providing more than two levels of encryption or decryption depending upon the derived cryptographic check value. In this arrangement, check value generator 7 creates a number of further comparison check values S' from the derived encryption key K using plural certification functions h. Comparator 8 compares

the derived check value S and the further comparison check values S' and outputs as signal b a signal indicating true or false in response to each check value comparison to selection means 12. Simultaneously with the signal b, check value generator 7 sends a signal j to selection means 12 which indicates the hash function h to which the particular signal b corresponds.

Selection means 12 uses function d to derive from signal b and signal j which hash function being tested has resulted in matching check values and outputs a signal i which indicates the encryption strength level corresponding to the matching check values. Encryption means 9 encrypts plain text communications using the derived encryption key K in accordance with the variable-strength encryption algorithm a, at the strength level indicated by the signal i.

An alternative way of coding and testing for multiple levels would be use to multiple hash keys instead of multiple hash algorithms h. In this case, a key or level number n could be passed from function h to a hash key store to request the hash key appropriate to the encryption strength level to be tested. Check value generator 7 would also pass the level information to selection means 12 by means of signal j. Selection means 12 could then record the value of the signal j for which signal b is true using function d and indicate this value to encryption means 9 by means of signal i. Encryption means 9 would then modify the strength of the encryption algorithm a to the level indicated by the signal i.

Although the above embodiments of the present invention have been described in relation to providing an input key with a check value and selecting the encryption strength on the basis of whether or not the input key derives the correct check value, as noted above, properties other than whether or not the input key derives a particular check value can be used to

select the encryption strength. For example, the derived key K_s could instead be divided by a particular number, and if the result of that division is an integer (i.e. the input key is divisible exactly by the particular number), then the encryption means controlled to provide strong encryption, but not otherwise. Alternatively, the derived key K_s could be compared with stored or calculated members of a particular mathematical series, and if a match is found strong encryption selected, but not otherwise.

Although the present invention has been described with particular reference to encryption, it is equally applicable to decryption, as will be appreciated by those skilled in the art. Such a decryption device would operate in the corresponding manner to the encryption device described above. Thus the decryption device would derive a decryption key and check value from an input cryptographic key and then use the derived decryption key to decrypt communications at a strength level selected in accordance with the derived check value. This arrangement would be particularly applicable in cases where the encryption device provides three or more levels of encryption strength. By inputting the input decryption key corresponding to the level of encryption used by the encryption device, the decryption device can be controlled to decrypt the encrypted message at the correct level of decryption strength.

In the case where cryptographic keys have been generated for use with the encryption device of the present invention or are to be generated in accordance with the present invention, and both an encryption key and a corresponding decryption key are desired, then the particular property (e.g. cryptographic check value) for the encryption key and the decryption key could be set to be identical, or could be set to be different (for example such that the encryption key has one check value

and the decryption key a different check value). In other words, the encryption and decryption keys could be treated in an identical manner, or could be considered completely separately, as desired. This applies equally whether the encryption and decryption keys are identical (such as might be the case in secret key cryptography), or differ (such as for public key cryptography). In the latter case, for example, the same cryptographic hash function could be used to derive check values (which would differ) for the public and private keys. In the case where the check values or particular properties differ for the distributed encryption and decryption keys, then, as will be appreciated, the check values or properties should derive the same levels of encryption/decryption strength.

The encryption apparatus of the present invention could be incorporated, *inter alia*, in any communication device which can provide encrypted communication, such as radios, telephones, etc.

Claims

1. A method of encrypting or decrypting communications comprising:

deriving from a first cryptographic key a cryptographic encryption key for use to encrypt or decrypt communications;

determining whether the first cryptographic key has a particular property;

selecting a level of encryption strength on the basis of the determination; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

2. The method of claim 1, wherein the derived encryption key differs from the first cryptographic key.

3. The method of claim 1 or 2, wherein the particular property according to which the encryption strength is selected is one of the following: whether or not the first cryptographic key includes a particular sequence of bits; whether or not the first cryptographic key is exactly divisible by a particular number; or whether or not the first cryptographic key belongs to a particular mathematical series.

4. The method of claim 1 or 2, wherein the particular property according to which the encryption strength is selected is whether or not an appropriate cryptographic check value is derivable from the first cryptographic key.

5. The method of claim 4, further comprising the step of deriving a cryptographic check value from the first cryptographic key, and wherein the level of encryption strength is selected on the basis of the derived check

value.

6. The method of claim 5, wherein the derived check value is compared with one or more other check values and the encryption strength selected on the basis of that comparison.

7. The method of claim 6, further comprising deriving from the first cryptographic key the other check value or values for comparison with the derived check value.

8. The method of claim 7, wherein the other check value or values is derived from the first cryptographic key by performing a predetermined cryptographic function on the derived encryption key.

9. The method of claim 8, wherein the predetermined cryptographic function is an irreversible cryptographic hash function.

10. The method of any one of the preceding claims, wherein a higher level of encryption strength is selected if the first cryptographic key has the particular property, and encryption of a lower strength is selected if the first cryptographic key does not have the particular property.

11. The method of any one of the preceding claims, wherein the encryption strength to be used is selected from three or more different levels of encryption strength on the basis of the determination.

12. The method of any one of the preceding claims, further including a step of deriving the first encryption key by decrypting another encrypted cryptographic key.

13. An encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for deriving from a cryptographic key input by a user of the apparatus a cryptographic encryption key for use to encrypt or decrypt communications;

means for determining whether the input cryptographic key has a particular property;

means for selecting one of said two or more levels of encryption strength on the basis of the determination; and

means for encrypting or decrypting communications at the selected level of encryption strength using the derived encryption key.

14. The apparatus of claim 13, wherein the particular property according to which the encryption strength is selected is whether or not an appropriate cryptographic check value is derivable from the input cryptographic key.

15. The apparatus of claim 14, further comprising means for deriving a cryptographic check value from the input cryptographic key, and wherein the level of encryption strength is selected on the basis of the derived check value.

16. The apparatus of claim 15, further comprising means for comparing the derived check value with one or more other check values and for selecting the encryption strength on the basis of that comparison.

17. The apparatus of claim 16, further comprising means for deriving from the first cryptographic key the other check value or values for comparison with the derived check value.

18. The apparatus of any one of claims 13 to 17,

further comprising means for decrypting the input cryptographic key, and wherein the means for deriving a cryptographic encryption key comprises means for deriving a cryptographic encryption key from the decrypted input cryptographic key, and the means for determining whether the input cryptographic key has a particular property comprises means for determining whether the decrypted input cryptographic key has a particular property.

19. A method of encrypting or decrypting communications comprising:

deriving from a cryptographic key a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

selecting a level of encryption strength on the basis of the derived check value; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

20. An encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for deriving from a cryptographic key input by a user of the apparatus a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

means for selecting one of said two or more levels of encryption strength on the basis of the derived check value; and

means for encrypting or decrypting communications at the selected level of encryption strength using the derived encryption key.

21. A method of encrypting or decrypting communications, comprising:

deriving from a cryptographic key a cryptographic

encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

deriving from the derived encryption key a further cryptographic check value;

comparing the derived check value and the further check value;

selecting a level of encryption strength on the basis of the comparison; and

using the derived encryption key to encrypt or decrypt communications at the selected level of encryption strength.

22. An encryption apparatus which can provide two or more levels of encryption strength, comprising:

means for deriving from a cryptographic key input by a user of the apparatus a cryptographic encryption key for use to encrypt or decrypt communications, and a cryptographic check value;

means for deriving from the derived encryption key a further cryptographic check value;

means for comparing the derived check value and the further check value;

means for selecting one of said two or more levels of encryption strength on the basis of the comparison; and

means for encrypting or decrypting communications at the selected level of encryption strength using the derived encryption key.

23. A method of generating a cryptographic key having a check value for authorising its validity, comprising:

generating an encryption key for use to encrypt or decrypt communications;

generating a check value from the encryption key by performing one or more cryptographic functions on the encryption key; and

combining the encryption key and check value to

form a certificated cryptographic key.

24. The method of claim 23, further comprising the step of encrypting the certificated cryptographic key.

25. An apparatus for generating a cryptographic key having a check value for authorising its validity, comprising:

means for generating an encryption key for use to encrypt or decrypt communications;

means for generating a check value from the encryption key by performing one or more cryptographic functions on the encryption key; and

means for combining the encryption key and check value to form a certificated cryptographic key.

26. The apparatus of claim 25, further comprising means for encrypting the certificated cryptographic key.

27. A method of encrypting or decrypting communications substantially as hereinbefore described with reference to any of the accompanying drawings.

28. Apparatus for encrypting or decrypting communications substantially as hereinbefore described with reference to any of the accompanying drawings

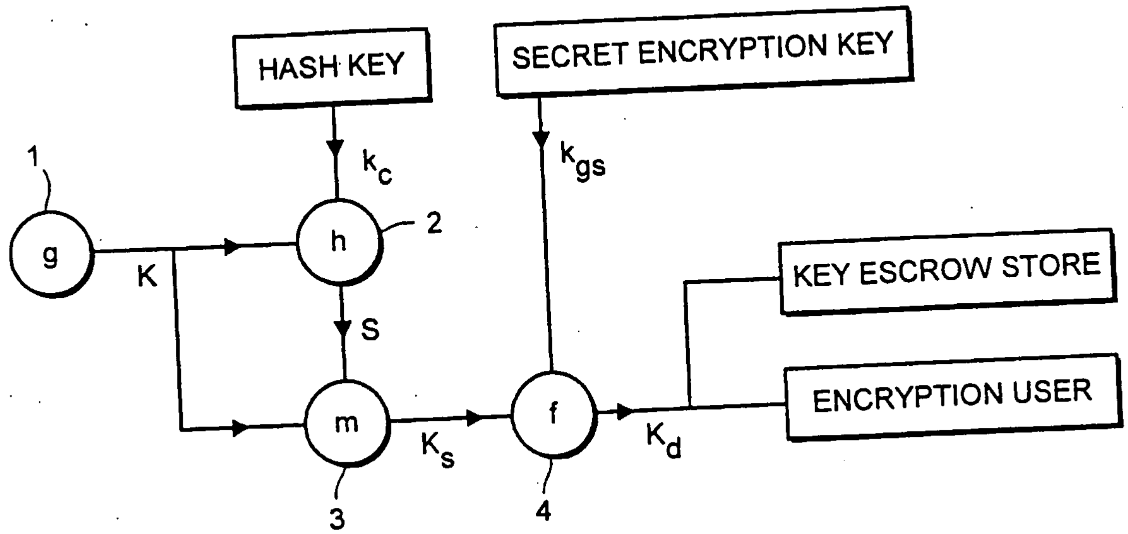

HASH KEY
SECRET ENCRYPTION KEY
k_c
k_{gs}
1
g
K
h
2
S
m
3
K_s
f
4
K_d
KEY ESCROW STORE
ENCRYPTION USER

FIG. 1

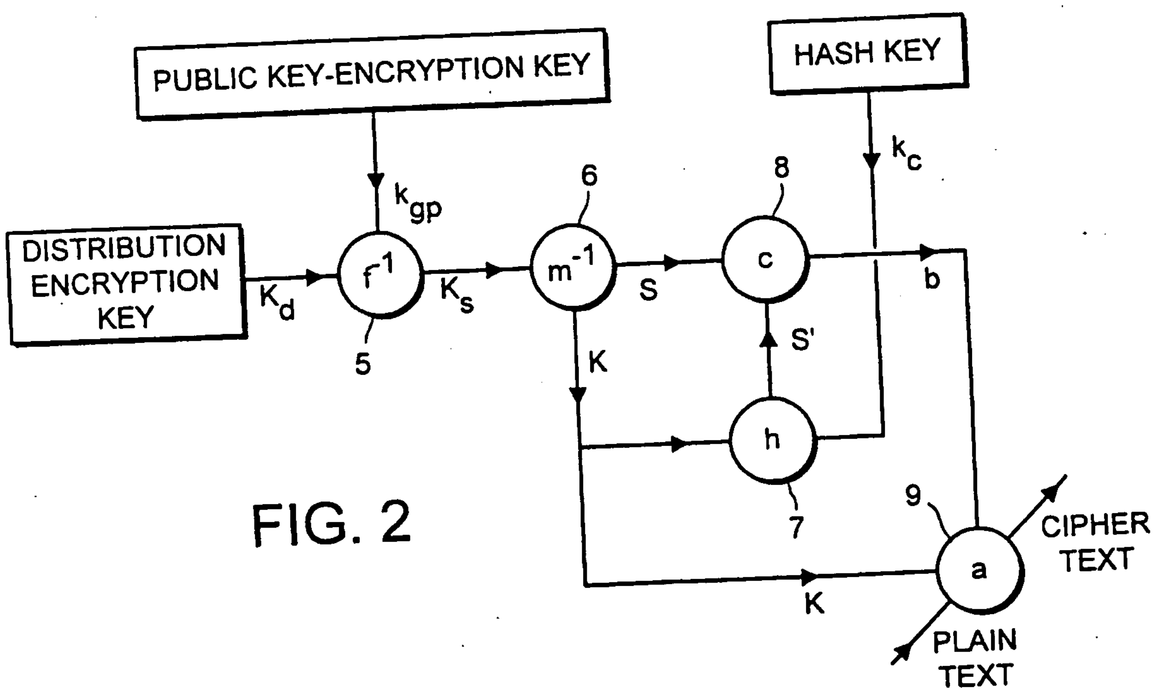

PUBLIC KEY-ENCRYPTION KEY
HASH KEY
k_{gp}
k_c
DISTRIBUTION ENCRYPTION KEY
K_d
f^{-1}
5
K_s
m^{-1}
6
S
c
8
b
S'
K
h
7
9
a
K
CIPHER TEXT
PLAIN TEXT

FIG. 2

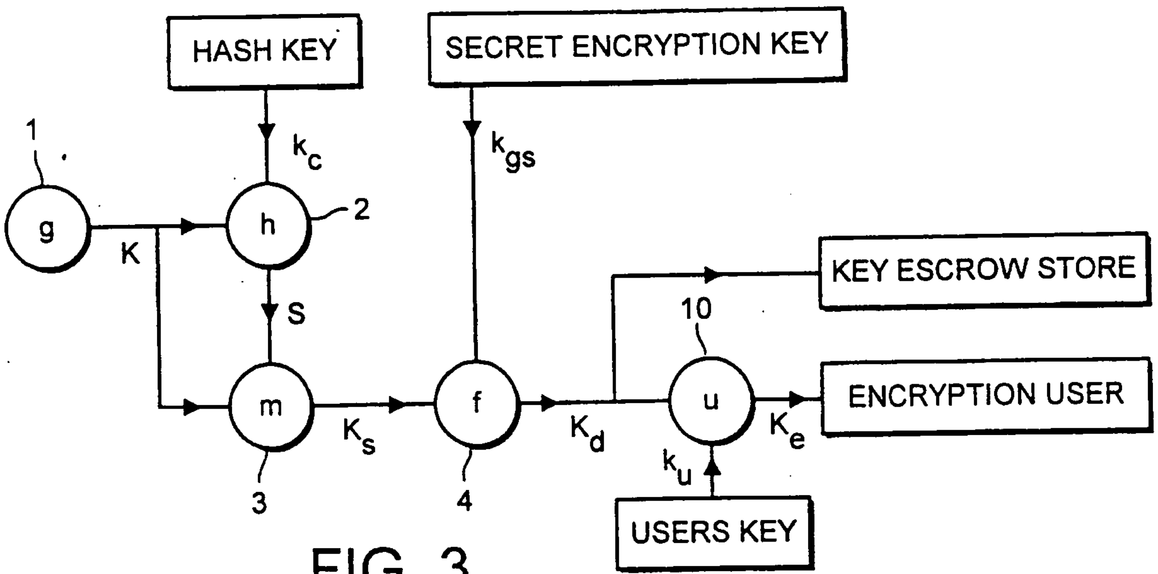

HASH KEY
SECRET ENCRYPTION KEY
k_c
k_{gs}
1
g
h
2
K
S
KEY ESCROW STORE
10
m
f
u
ENCRYPTION USER
K_s
K_d
K_e
k_u
3
4
USERS KEY

FIG. 3

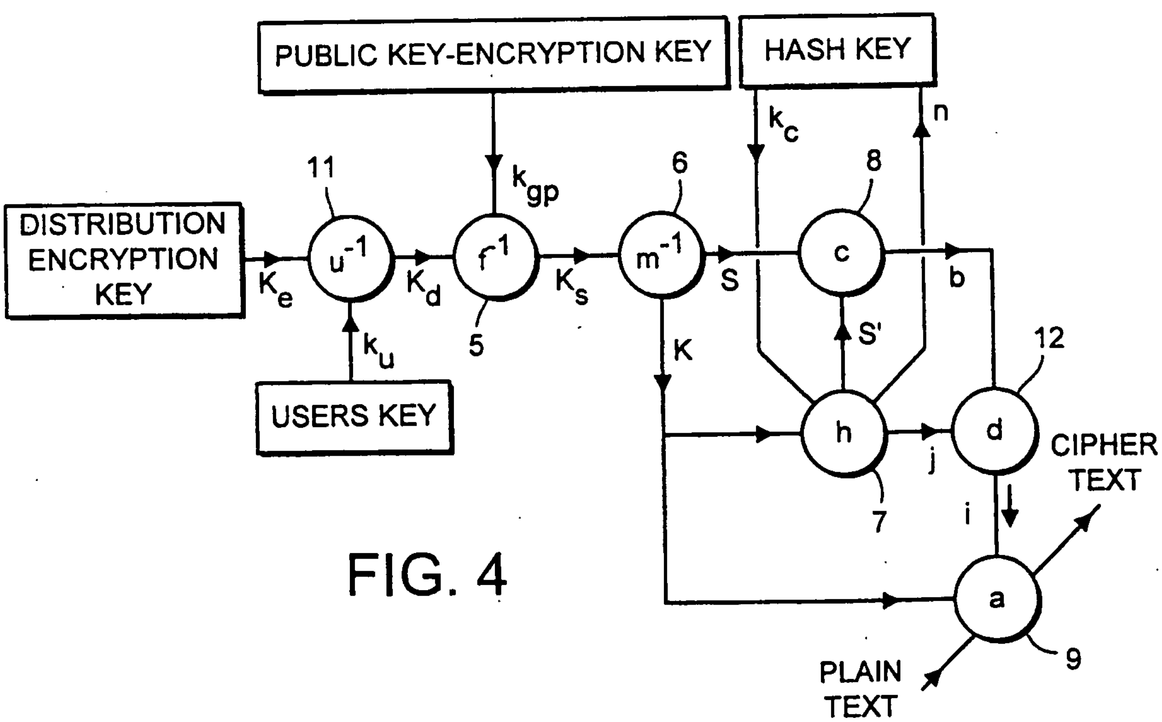

PUBLIC KEY-ENCRYPTION KEY
HASH KEY
k_c
n
11
k_{gp}
6
8
DISTRIBUTION ENCRYPTION KEY
u^{-1}
f^{-1}
m^{-1}
c
K_e
K_d
K_s
S
b
k_u
5
K
S'
12
USERS KEY
h
d
CIPHER TEXT
j
7
i
a
9
PLAIN TEXT

FIG. 4

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/GB 98/02774

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 729 252 A (INT COMPUTERS LTD) 28 August 1996 see page 2, line 9 - line 28 see page 3, line 40 - page 4, line 31 see page 6, line 8 - line 48 see page 7, line 13 - line 31	1-3,10, 12,13, 18-20
X	US 5 073 934 A (MATYAS STEPHEN M ET AL) 17 December 1991	23,25
A	see column 9, line 54 - column 11, line 52	1-4,13, 14,19,20

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 January 1999	18/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 98/02774

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0729252 A	28-08-1996	US 5745572 A	28-04-1998
US 5073934 A	17-12-1991	DE 69111556 D	31-08-1995
		DE 69111556 T	07-03-1996
		EP 0482371 A	29-04-1992
		JP 2575558 B	29-01-1997
		JP 4265031 A	21-09-1992